

Contextual Entropy and Reconstruction of Quantum States

Carmen Maria Constantin, Andreas Döring

Quantum Group, Department of Computer Science, Oxford University, Oxford

(Dated: August 13, 2012)

We introduce a new notion of entropy for quantum states, called contextual entropy, and show how it unifies Shannon and von Neumann entropy. The main result is that from the knowledge of the contextual entropy of a quantum state of a finite-dimensional system, one can reconstruct the quantum state, i.e., the density matrix, if the Hilbert space is of dimension 3 or greater. We present an explicit algorithm for this state reconstruction and relate our result to Gleason's theorem.

PACS numbers: 03.67.-a

INTRODUCTION

Quantum Information Theory has brought the importance of information-theoretic concepts to the forefront of physics. Quantum systems have been shown to be able to perform information-theoretic tasks beyond the capabilities of classical systems, e.g. secure key commitment [1], quantum teleportation [2], factoring primes in polynomial time [3], and many others. Here, we will compare quantum systems to classical systems at the level of their associated information-theoretic notions, in particular we consider *entropy* of physical states. For classical states, Shannon entropy [4] is typically used, for quantum states, von Neumann entropy [5]. We will show how a new notion of contextual entropy unifies these two.

Let ρ be a quantum state. In the following, we will distinguish between the (fixed and basis-independent) state ρ itself and the basis-dependent density matrix $\tilde{\rho}$ representing it. The von Neumann entropy $S(\rho)$ of ρ is the Shannon entropy of a specific probability distribution, given by the diagonal elements of $\tilde{\rho}$ in a basis in which $\tilde{\rho}$ is diagonal. Picking such an orthonormal basis means choosing a particular measurement context. Yet, infinitely many other measurement contexts (in which $\tilde{\rho}$ typically is not a diagonal matrix) are available and have a well-defined operational meaning.

In this article, we show that it is fruitful to take all possible measurement contexts into account and consider a family of Shannon entropies, one for each context. This leads to the new notion of the contextual entropy of a quantum state, which is a real-valued function from which the density matrix $\tilde{\rho}$ and hence the state ρ can be reconstructed. This also provides an extension of Gleason's theorem.

DEFINITION OF CONTEXTUAL ENTROPY

Consider a finite-dimensional quantum system with Hilbert space $\mathcal{H} = \mathbb{C}^n$, for example a spin system, or a system of m qubits, in which case $n = 2^m$. Let $(\hat{P}_1, \dots, \hat{P}_k)$ be a family of projection operators on \mathcal{H} such that $\hat{P}_i \hat{P}_j = \delta_{ij} \hat{P}_i$ and $\sum_{i=1}^k \hat{P}_i = \hat{1}$. Such a family is called a *context* (or sometimes a *resolution of the identity*) and describes a measurement with k out-

comes. Conceptually, a measurement context is a 'classical perspective' on the quantum system. A context $C := (\hat{P}_1, \dots, \hat{P}_k)$ can be interpreted as the family of projections onto the eigenspaces of an observable of the form $\hat{A} = \sum_{i=1}^k a_i \hat{P}_i$ with k distinct real eigenvalues a_i . The a_i are not determined by the \hat{P}_i (and their actual numerical values do not matter).

Given a context $C = (\hat{P}_1, \dots, \hat{P}_k)$, we can obtain coarse-grained contexts by introducing degeneracy: for example, $C' = (\hat{P}_1 + \hat{P}_2, \hat{P}_3, \dots, \hat{P}_k)$ is another context in which the outcomes 1 and 2 cannot be distinguished. We write $C' \leq C$ if each projection in C' is either in C or is the sum of projections in C , and every projection in C shows up in such a sum exactly once. In this case we say that the context C' is *coarser* (or *more degenerate*) than the context C . This gives a partial order on the set \mathcal{C} of all contexts of our quantum system.

A context C is called *maximal* if there are no contexts $\tilde{C} \neq C$ such that $C \leq \tilde{C}$. If $C = (\hat{P}_1, \dots, \hat{P}_n)$ is maximal, then the n projections \hat{P}_i are of rank 1 and C corresponds to a non-degenerate measurement. Each rank-1 projection \hat{P}_i determines a unit vector $|\psi_i\rangle$ such that $|\psi_i\rangle\langle\psi_i| = \hat{P}_i$. This vector is unique up to a phase. Hence, with each maximal context we can associate an orthonormal basis $(|\psi_1\rangle, \dots, |\psi_n\rangle)$ of \mathcal{H} that is unique up to phases. If $C = (\hat{P}_1, \dots, \hat{P}_k)$ with $k < n$ is a non-maximal context, one can still find a (non-unique) orthonormal basis of \mathcal{H} such that all the \hat{P}_i in C are given by diagonal matrices with respect to this basis, since all the projections in C commute.

Not all contexts $C, \tilde{C} \in \mathcal{C}$ can be compared with respect to the order defined above. This corresponds to the fact that some measurements are incompatible. However, incompatible contexts can be coarse-grained to the same context C . Consider for example the three spin operators \hat{S}_i in $\mathcal{H} = \mathbb{C}^2$. Each \hat{S}_i defines a context C_i , given by the two projections onto the eigenspaces of \hat{S}_i . As is well-known, the \hat{S}_i do not commute, but they all commute with the total spin $\hat{\mathbf{S}}^2$. The latter defines a context C that just contains the identity operator $\hat{1}$ and hence is coarser than C_1, C_2 and C_3 . This indicates that the partial order gives a rich structure to the set \mathcal{C} of all contexts. For some results on the structure of \mathcal{C} see [6, 7].

Let ρ be a state of a finite-dimensional quantum system, described by a density matrix $\tilde{\rho}$. We will say that ρ is *diagonal in a context* $C = (\hat{P}_1, \dots, \hat{P}_k)$ if ρ is of the form $\rho = \sum_{i=1}^k \lambda_i \hat{P}_i$. This is justified by the following: if $\mathcal{B} = (|\psi_1\rangle, \dots, |\psi_n\rangle)$ is an orthonormal basis of \mathcal{H} such that all projections \hat{P}_i in C are given by diagonal matrices with respect to \mathcal{B} , then $\tilde{\rho}$ is diagonal with respect to \mathcal{B} if and only if $\rho = \sum_i \lambda_i \hat{P}_i$.

Given a measurement with k outcomes described by a context C , the quantum state ρ assigns a probability $p_i := \text{Prob}(i; \rho) = \text{tr}(\tilde{\rho} \hat{P}_i)$ to each outcome $i = 1, \dots, k$. This defines a probability distribution $P_C := (p_1, \dots, p_k)$. Since a context can be interpreted as a *classical perspective* on a quantum system, it makes sense to assign a (classical) Shannon entropy to the probability distribution P_C , which is $H(P_C) = -\sum_{i=1}^k p_i \ln p_i$. Yet, no context C is preferred over the others, so we consider *all* contexts $C \in \mathcal{C}$. This gives a map

$$E_\rho : \mathcal{C} \longrightarrow [0, \ln n]$$

$$C = (\hat{P}_1, \dots, \hat{P}_k) \longmapsto H(P_C) = H(\text{tr}(\tilde{\rho} \hat{P}_1), \dots, \text{tr}(\tilde{\rho} \hat{P}_k)).$$

Here, $[0, \ln n]$ denotes the real interval from 0 to $\ln n$. The map E_ρ is called the *contextual entropy* of the quantum state ρ . It is a family of Shannon entropies, one for each context $C \in \mathcal{C}$.

PROPERTIES OF CONTEXTUAL ENTROPY

We show two important properties of contextual entropy. The first of these highlights the connection between the von Neumann and the contextual entropy of a state and will be useful for our reconstruction algorithm. The second one shows that the contextual entropy is a monotone map.

Von Neumann entropy from contextual entropy. We first show that there exists at least one maximal context $C_\rho \in \mathcal{C}$ such that $E_\rho(C_\rho) = S(\rho)$, the von Neumann entropy of the state ρ : let $C_\rho = (\hat{P}_1, \dots, \hat{P}_n)$ be a maximal context in which ρ is diagonal, that is, $\rho = \sum_{i=1}^n \lambda_i \hat{P}_i$. Then $P_{C_\rho} = (\text{tr}(\tilde{\rho} \hat{P}_1), \dots, \text{tr}(\tilde{\rho} \hat{P}_n)) = (\lambda_1, \dots, \lambda_n)$ and hence $E_\rho(C_\rho) = H(P_{C_\rho}) = -\sum_i \lambda_i \ln \lambda_i = S(\rho)$, which is what we wanted to show.

Secondly, recall that a vector $\mathbf{r} = (r_1, \dots, r_n)$ of real numbers is *majorised* by another real vector $\mathbf{s} = (s_1, \dots, s_n)$ if $\sum_{i=1}^n r_i = \sum_{i=1}^n s_i$ and, for all $k < n$, $\sum_{i=1}^k r_i^\downarrow \leq \sum_{i=1}^k s_i^\downarrow$, where the r_i^\downarrow are the components of \mathbf{r} rearranged in decreasing order, and similarly for the s_i^\downarrow [8].

Using the majorisation order, we can show a stronger result: the von Neumann entropy $S(\rho)$ of a quantum state ρ is the *minimal* value of the contextual entropy $E_\rho(C)$ when C is varying over maximal contexts.

To see this, let $C = (\hat{P}_1, \dots, \hat{P}_n)$ be any maximal context. Necessarily, all projections $\hat{P}_i \in C$ are of rank

1. Consider the matrix representation of \hat{P}_i with respect to the orthonormal basis $\mathcal{B}_C = (|\psi_1\rangle, \dots, |\psi_n\rangle)$ associated with the context C . This matrix has a single 1 in position (i, i) and zeros everywhere else. Then $p_i = \text{tr}(\tilde{\rho} \hat{P}_i) = \text{tr}(\tilde{\rho} \hat{P}_i^2) = \text{tr}(\hat{P}_i \tilde{\rho} \hat{P}_i)$ is the i th diagonal element of the density matrix $\tilde{\rho}$ when written with respect to the basis \mathcal{B}_C . Hence, the probability distribution $P_C = (p_1, \dots, p_n)$ in context C determined by the state ρ consists of the diagonal elements of the density matrix $\tilde{\rho}$ when the latter is written with respect to the basis \mathcal{B}_C associated with C .

The Schur-Horn theorem [9] states that the vector $\mathbf{l} = (\lambda_1, \dots, \lambda_n)$ of eigenvalues of a Hermitian diagonal matrix M majorises the vector $\mathbf{k} = (\kappa_1, \dots, \kappa_n)$ of diagonal elements of the Hermitian matrix $\hat{U} M \hat{U}^{-1}$ obtained after a change of basis. In our situation, $M = \tilde{\rho}$, and a change of basis amounts to a change of maximal context. So, if $C_\rho = (\hat{Q}_1, \dots, \hat{Q}_n)$ is a maximal context in which ρ is diagonal and C is any other maximal context, then the vector $P_{C_\rho} = (\lambda_1, \dots, \lambda_n)$ of eigenvalues of ρ majorises the vector $P_C = (p_1, \dots, p_n)$ of diagonal elements of $\tilde{\rho}$ written with respect to the basis associated with C .

It is well-known that the Shannon entropy reverses the majorisation order, so it follows that the contextual entropy E_ρ takes its minimal value on the set of maximal contexts of the form C_ρ for which $\tilde{\rho}$ is a diagonal matrix. We saw above that for such contexts C_ρ , the value $E_\rho(C_\rho)$ of the contextual entropy is the von Neumann entropy $S(\rho)$ of the quantum state. This completes the proof.

Monotonicity. Now consider two contexts $C, C' \in \mathcal{C}$ such that C' is coarser than C . We want to compare $E_\rho(C')$ and $E_\rho(C)$. Let $C' = (\hat{P}_1, \dots, \hat{P}_k)$, and let $C = (\hat{Q}_1^1, \dots, \hat{Q}_{l_1}^1, \hat{Q}_1^2, \dots, \hat{Q}_{l_2}^2, \dots, \hat{Q}_1^k, \dots, \hat{Q}_{l_k}^k)$, where $\sum_{j=1}^{l_i} \hat{Q}_j^i = \hat{P}_i$ for all $i = 1, \dots, k$. Given a quantum state ρ , we have $p_i = \text{tr}(\tilde{\rho} \hat{P}_i) = \text{tr}(\tilde{\rho} \hat{Q}_1^i) + \dots + \text{tr}(\tilde{\rho} \hat{Q}_{l_i}^i)$ for all $i = 1, \dots, k$. Let us denote $q_j^i := \text{tr}(\tilde{\rho} \hat{Q}_j^i)$, where $i = 1, \dots, k$ and $j = 1, \dots, l_i$. Then, using the recursion property of Shannon entropy (see e.g. [10]),

$$\begin{aligned} E_\rho(C) &= H(q_1^1, \dots, q_{l_1}^1, q_1^2, \dots, q_{l_2}^2, \dots, q_1^k, \dots, q_{l_k}^k) \\ &= H(p_1, \dots, p_k) + \sum_{i=1}^k p_i H\left(\frac{q_1^i}{p_i}, \dots, \frac{q_{l_i}^i}{p_i}\right) \\ &= E_\rho(C') + \sum_{i=1}^k p_i H\left(\frac{q_1^i}{p_i}, \dots, \frac{q_{l_i}^i}{p_i}\right). \end{aligned}$$

Since the last term above is always non-negative, it follows that $E_\rho(C') \leq E_\rho(C)$ for all contexts $C' \leq C$. Hence, the map $E_\rho : \mathcal{C} \rightarrow [0, \ln n]$ is indeed order-preserving.

RECONSTRUCTION OF QUANTUM STATES

We now show that the contextual entropy of a quantum state ρ contains enough information to uniquely re-

construct the density matrix $\tilde{\rho}$ if the dimension of the Hilbert space is at least 3. We assume that we can identify a maximal context C_ρ for which E_ρ takes its minimal value among all maximal contexts. (In general, the minimal value of E_ρ will be attained in many different maximal contexts, but any of them will do.) We remark in passing that the same reconstruction algorithm would also work for contextual Rényi entropies.

Pure states. Assume that ρ is pure, i.e., $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$. We want to determine $|\psi\rangle\langle\psi|$ from the contextual entropy E_ρ .

We first note that a state ρ is pure if and only if $E_\rho(C_\rho) = 0$. This follows from the previous section, where we showed that $E_\rho(C_\rho) = S(\rho)$, the von Neumann entropy of ρ . The latter is equal to 0 if and only if ρ is a pure state.

Let $C = (\hat{P}_1, \dots, \hat{P}_n)$ be a context for which $E_\rho(C) = 0$. Then there is a unique $\hat{P}_{i_0} \in C$ such that $|\psi\rangle\langle\psi| = \hat{P}_{i_0}$. Using finitely many values of the contextual entropy E_ρ , it is possible to determine which of the n projections $\hat{P}_1, \dots, \hat{P}_n$ equals $|\psi\rangle\langle\psi|$. For this, consider n unitary matrices $\hat{U}_1, \dots, \hat{U}_n$ such that $\hat{U}_i \hat{P}_i \hat{U}_i^{-1} = \hat{P}_i$ and, for all $1 \leq j \leq n$, $j \neq i$,

$$\hat{U}_i \hat{P}_j \hat{U}_i^{-1} \notin \{\hat{P}_1, \dots, \hat{P}_n\}.$$

That is, \hat{U}_i leaves the projection \hat{P}_i invariant and ‘rotates’ the other projections \hat{P}_j , $j \neq i$ without resulting in a permutation of any of them. Such unitaries always exist if $\dim \mathcal{H} \geq 3$: for example, a unitary keeping \hat{P}_1 fixed and rotating all other \hat{P}_j has a matrix of the form

$$\hat{U} = \left(\begin{array}{c|c} 1 & \mathbf{0}^T \\ \hline \mathbf{0} & \hat{U}' \end{array} \right),$$

where the unitary $\hat{U}' \in \mathcal{U}(n-1)$ can be taken to be a rotation by some small angle around an axis different from all the $n-1$ coordinate directions for $j = 2, \dots, n$.

Consider the maximal contexts of the form $C_i := (\hat{U}_i \hat{P}_1 \hat{U}_i^{-1}, \dots, \hat{U}_i \hat{P}_n \hat{U}_i^{-1})$ for $i = 1, \dots, n$. Only the context C_{i_0} contains the projection $\hat{P}_{i_0} = |\psi\rangle\langle\psi|$, which is the state that we are looking for. Hence, the density matrix $\tilde{\rho}$ is only diagonal with respect to the orthonormal basis associated with the maximal context C_{i_0} , while it is not diagonal with respect to the bases associated with any of the contexts C_j , $j \neq i_0$. If the density matrix $\tilde{\rho}$ of a projection $|\psi\rangle\langle\psi|$ is not diagonal with respect to some basis, then there are at least two non-zero entries on the diagonal, so the probability distribution (p_1, \dots, p_n) given by the diagonal elements of $\tilde{\rho}$ has Shannon entropy strictly larger than 0.

Hence, $E_\rho(C_{i_0}) = 0$, while $E_\rho(C_j) > 0$ for all $j \neq i_0$. In this way, we can identify i_0 and can determine the state $|\psi\rangle\langle\psi|$.

Mixed states. We now show how to reconstruct $\tilde{\rho}$ from E_ρ when ρ is a mixed state and $\dim \mathcal{H} \geq 3$.

Step 1. Find a maximal context $C_\rho = (\hat{P}_1, \dots, \hat{P}_n)$ for which the value $E_\rho(C_\rho)$ is minimal (but larger than 0 since ρ is mixed). The Schur-Horn theorem implies that the state which we want to determine is diagonal in C_ρ , that is, $\rho = \sum_{i=1}^n \lambda_i \hat{P}_i$. We have to find the eigenvalues λ_i of ρ .

Step 2. Let $C_i := (\hat{P}_i, \hat{1} - \hat{P}_i)$ be the context containing just \hat{P}_i and its complement, for each $i = 1, \dots, n$. Then $E_\rho(C_i)$ is the Shannon entropy of the probability distribution $(\text{tr}(\tilde{\rho} \hat{P}_i), 1 - \text{tr}(\tilde{\rho} \hat{P}_i))$.

Of course, the actual values $\lambda_i := \text{tr}(\tilde{\rho} \hat{P}_i)$ and $1 - \lambda_i = 1 - \text{tr}(\tilde{\rho} \hat{P}_i)$ are unknown so far. We just have the binary entropy

$$E_\rho(C_i) = -x_i \ln x_i - (1 - x_i) \ln(1 - x_i).$$

Solving this, we obtain two solutions, c_i and $1 - c_i$. We can assume without loss of generality that $c_i \leq \frac{1}{2} \leq 1 - c_i$. For each i , the eigenvalue λ_i of the density matrix $\tilde{\rho}$ is either c_i or $1 - c_i$.

Step 3. We write the solutions c_1, \dots, c_n and $1 - c_1, \dots, 1 - c_n$ in two rows such that $1 - c_i$ is beneath c_i . In order to find the eigenvalues λ_i of the density matrix $\tilde{\rho} = \sum_{i=1}^n \lambda_i \hat{P}_i$, written with respect to the basis associated with C_ρ , we must choose n numbers from this table, one from each column, such that their sum is equal to 1 (since $\sum_{i=1}^n \lambda_i = 1$). At least one such solution must exist, since we assumed that E_ρ is the contextual entropy of some quantum state ρ .

(a) If the numbers c_i in the top row add up to 1, then we have found the unique solution: $\lambda_i := c_i$ for each $i = 1, \dots, n$. Picking any $1 - c_i$ instead of c_i would make the total sum greater than 1.

(b) If the sum $S := \sum_{i=1}^n c_i$ of the elements in the top row is smaller than 1, then we must replace at least one value c_j from the top row with $1 - c_j$ from the bottom row. Note, however, that since the entries of the bottom row are all greater or equal to $\frac{1}{2}$, we can only pick exactly one such entry, since picking two or more would make the sum of our n chosen elements greater than 1.

To determine which c_j (from the top row) must be replaced by $1 - c_j$ (from the bottom row) among the n elements we pick, we note the following: the sum $c_1 + \dots + c_{j-1} + (1 - c_j) + c_{j+1} + \dots + c_n$ must equal 1, which implies that c_j must have the value $c := \frac{(c_1 + \dots + c_n)}{2} = \frac{S}{2} < \frac{1}{2}$.

(b1) If the value c appears only once among the entries of the top row, for example in the j th column, then our unique solution is $\lambda_j = 1 - c_j$ and $\lambda_i = c_i$ for all $i \neq j$.

(b2) If, however, the value c appears twice among the entries of the top row, the bottom row has $1 - c$ in the corresponding two columns. This implies that the top row has 0s in all other columns, since otherwise the sum of $1 - c$ (the unique entry picked from the bottom row) and the sum of the $n - 1$ entries from the other columns of the top row would be larger than 1. This also implies that c cannot appear three or more times among the entries

of the top row. Assume that the two entries of c appear in the j th and k th columns. Our state is then either

$$\rho = c\hat{P}_j + (1 - c)\hat{P}_k \quad (1)$$

or

$$\rho = c\hat{P}_k + (1 - c)\hat{P}_j. \quad (2)$$

In order to determine which of these is the correct solution, consider a unitary \hat{U} which rotates, but does not permute, all the projections $\hat{P}_1, \dots, \hat{P}_n$ except for \hat{P}_j , which it leaves unchanged. Here, we need $\dim \mathcal{H} \geq 3$. The j th eigenvalues of $\hat{U}^{-1}\rho\hat{U}$ and ρ (that is, the eigenvalues for the joint eigenvector determined by \hat{P}_j) coincide and are equal to λ_j , while the other eigenvalues are distinct in general. We consider the contexts of the form $W_i = (\hat{U}\hat{P}_i\hat{U}^{-1}, \hat{1} - \hat{U}\hat{P}_i\hat{U}^{-1})$ and solve the equations

$$E_\rho(W_i) = -d_i \ln d_i - (1 - d_i) \ln(1 - d_i).$$

We write the solutions in a second table, again with the convention that the top row contains entries smaller than $\frac{1}{2}$. We then repeat the procedure detailed above (from **Step 3** onwards) of choosing n numbers adding up to 1, this time from the second table. These numbers will be equal to the diagonal entries of the matrix $\hat{U}^{-1}\tilde{\rho}\hat{U}$, written in the basis in which $\tilde{\rho}$ is diagonal.

Because of our choice of unitary, the diagonal entries of the density matrix $\hat{U}^{-1}\tilde{\rho}\hat{U}$ will contain at least three non-zero elements, so we do not enter the **(b2)** branch of our algorithm again, since the top row of the second table will also contain at least three non-zero entries. Hence, this time there will be a unique choice of n entries adding up to 1. In particular, the j th element of this solution equals the j th diagonal entry of the matrix $\hat{U}^{-1}\tilde{\rho}\hat{U}$, which is the same as λ_j , the j th eigenvalue of ρ . This allows us to choose the correct quantum state from the two possible solutions (1) and (2). We finally remark that for $\dim \mathcal{H} = 2$, the qubit case, we can determine the state up to the ambiguity between (1) and (2).

RELATION TO GLEASON'S THEOREM

Let $\mathcal{H} = \mathbb{C}^n$, $n \geq 3$, and let μ be a (finitely additive) probability measure $\mu : \mathcal{P}(\mathcal{H}) \rightarrow [0, 1]$ on the projections of \mathcal{H} , that is $\mu(\hat{1}) = 1$ and if $\hat{P}\hat{Q} = \hat{Q}\hat{P} = \hat{0}$, then $\mu(\hat{P} + \hat{Q}) = \mu(\hat{P}) + \mu(\hat{Q})$.

Gleason's theorem [11] (which we only consider for the finite-dimensional case here) states that for every such probability measure μ , there exists a quantum state ρ_μ such that, for all projections $\hat{P} \in \mathcal{P}(\mathcal{H})$,

$$\text{tr}(\tilde{\rho}_\mu \hat{P}) = \mu(\hat{P}). \quad (3)$$

Conversely, every quantum state ρ gives a probability measure $\mu_\rho : \mathcal{P}(\mathcal{H}) \rightarrow [0, 1]$ simply by setting $\mu_\rho(\hat{P}) := \text{tr}(\tilde{\rho}\hat{P})$ for all $\hat{P} \in \mathcal{P}(\mathcal{H})$.

A probability measure μ defines a probability distribution $P_C = (\mu(\hat{P}_1), \dots, \mu(\hat{P}_k))$ for each context $C = (\hat{P}_1, \dots, \hat{P}_k)$. Gleason's theorem shows that if we have a

family $(P_C)_{C \in \mathcal{C}}$ of probability distributions, one for each context, that come from a measure μ , then there is a unique quantum state ρ_μ such that eq. (3) holds.

Given μ , we can construct the corresponding contextual entropy E_μ : to each context $C = (\hat{P}_1, \dots, \hat{P}_k)$, we assign the Shannon entropy of the probability distribution P_C . As was shown in the previous section, one can reconstruct the quantum state ρ_μ from its contextual entropy E_μ . This requires a *single* real number $E_\mu(C)$ for each context $C = (\hat{P}_1, \dots, \hat{P}_k)$ instead of the k numbers $\mu(\hat{P}_1), \dots, \mu(\hat{P}_k)$. Moreover, we obtain an explicit density matrix from our reconstruction, while Gleason's theorem merely shows that a density matrix must exist. In this sense, our approach via the contextual entropy is an extension of Gleason's result.

On the other hand, Gleason's theorem guarantees that *every* probability measure $\mu : \mathcal{P}(\mathcal{H}) \rightarrow [0, 1]$ corresponds to a quantum state, while we had to assume that the map $E_\rho : \mathcal{C} \rightarrow [0, \ln n]$ which we use in our reconstruction actually is the contextual entropy of some quantum state.

SUMMARY AND OUTLOOK

Given a quantum state ρ on a finite-dimensional Hilbert space \mathcal{H} and a measurement context $C = (\hat{P}_1, \dots, \hat{P}_n)$, we can extract the probability distribution $P_C = (\text{tr}(\tilde{\rho}\hat{P}_1), \dots, \text{tr}(\tilde{\rho}\hat{P}_n))$ by repeated preparations and measurements. In contrast to the quantum state itself, measurement contexts have direct operational meaning. The contextual entropy $E_\rho : \mathcal{C} \rightarrow [0, \ln n]$, which is a real-valued function, assigns to each probability distribution P_C its Shannon entropy and hence encodes data that can be extracted operationally from the quantum state ρ .

The fact that the state ρ can be reconstructed from its contextual entropy E_ρ if $\dim \mathcal{H} \geq 3$ provides a new, information-theoretic characterisation of quantum states that takes contextuality into account explicitly. The results in this article connect directly with the so-called *topos approach* to quantum theory [12, 13] in which contextuality is a key concept. In future work, we will develop these connections in depth and will also consider infinite-dimensional systems.

We presented a number of properties of contextual entropy and discussed how the reconstruction of a quantum state from its contextual entropy relates to Gleason's theorem. As matters stand, the properties we presented do not characterise contextual entropy fully: there are functions $F : \mathcal{C} \rightarrow [0, \ln n]$ that have all the properties we discussed, but are not the contextual entropy of any quantum state.

Finding an axiomatic characterisation of exactly those functions which are contextual entropies of quantum states would, together with our reconstruction algorithm, provide an alternative proof of Gleason's theorem. This is an interesting and non-trivial open problem.

Acknowledgements. We thank Oscar Dahlsten, Andrei Constantin, Daniel Marsden, Rui Soares Barbosa and Chris Isham for discussions and suggestions, and we thank Samson Abramsky and Bob Coecke for support. C.M.C. is supported by an EPSRC graduate scholarship.

-
- [1] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 175–179 (1984).
 - [2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
 - [3] P. W. Shor, in *Proc. 35nd Annual Symposium on Foundations of Computer Science*, ed. Shafi Goldwasser, IEEE Computer Society Press, 124–134 (1994).
 - [4] C. E. Shannon, *Bell System Technical Journal* **27** (3), 379–423 (1948).
 - [5] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1955).
 - [6] J. Harding, A. Döring, arXiv:1009.4945 (2010).
 - [7] A. Döring and R. Soares Barbosa, in *Quantum Field Theory and Gravity*, eds. F. Finster, O. Müller, M. Nardmann, J. Tolksdorf, and E. Zeidler (Birkhäuser, Basel, 2011), 65–96.
 - [8] R. Bhatia, *Matrix Analysis* (Springer, New York, 1997).
 - [9] A. Horn, *Am. J. Math.* **76**, 620–630 (1954).
 - [10] Bengtsson, I., K. Życzkowski, *Geometry of Quantum States*, Cam. Univ. Press (2006)
 - [11] A. M. Gleason, *J. Mathematics and Mechanics* **6**, 885–893 (1957).
 - [12] A. Döring, C. J. Isham, *J. Math. Phys.* **49**, 053515, 16, 17 and 18 (2008).
 - [13] A. Döring, in *Quantum Field Theory, Competitive Models*, eds. B. Fauser, J. Tolksdorf, and E. Zeidler (Birkhäuser, Basel, 2009) 25–47.